

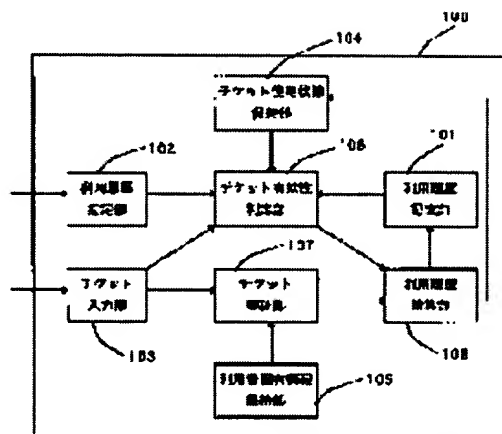
(11)Publication number : 11-224313
(43)Date of publication of application : 17.08.1999

G06K 17/00
G06F 17/60
G06K 19/10

(71)Applicant : FUJI XEROX CO LTD

(72)Inventor : NAKAGAKI JUHEI
KIKO KENICHIROU
KIYOUJIMA HITOKI
TANIGUCHI SHINICHIRO

A ticket verifying part 107 verifies the legality of the ticket while using the inputted ticket, user peculiar information, additional ticket information and ticket disclosure information. When the ticket validity discriminating part 106 discriminates the ticket is valid and the ticket verifying part 107 verifies the ticket is legal, a utilization history account settling part 108 regards the input of the legal ticket required for settling the account of the utilization history to which the settlement of account is designated, and the utilization history designated by the utilization history designating part 102 is regarded complete in the settlement of account.



[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-224313

(43)公開日 平成11年(1999) 8月17日

(51)Int.Cl.⁴
G 0 6 K 17/00

G 0 6 F 17/60
G 0 6 K 19/10

識別記号

F I
G 0 6 K 17/00 T
L
G 0 6 F 15/21 B
G 0 6 K 19/00 R

審査請求 未請求 請求項の数11 O L (全 13 頁)

(21)出願番号 特願平10-27143

(22)出願日 平成10年(1998) 2月9日

(71)出願人 000005496

富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者 中垣 寿平

神奈川県足柄上郡中井町境430 グリーン
テクなかい 富士ゼロックス株式会社内

(72)発明者 木子 健一郎

神奈川県足柄上郡中井町境430 グリーン
テクなかい 富士ゼロックス株式会社内

(72)発明者 京嶋 仁樹

神奈川県足柄上郡中井町境430 グリーン
テクなかい 富士ゼロックス株式会社内

(74)代理人 弁理士 澤田 俊夫

最終頁に続く

(54)【発明の名称】 電子チケットシステム

(57)【要約】

【課題】 利用時には、単に、その利用履歴を記録しておき、後に、種々のタイプのチケットを用いて精算する。

【解決手段】 チケット有効性判定部106は、使用状態保持部104に保持されているチケットの使用状態と、入力されたチケット付加情報と、利用履歴指定部102により指定された利用履歴とを用いてチケットの有効性を判定する。チケット検証部107は、入力されたチケットと利用者固有情報とチケット付加情報とチケット公開情報とを用いてチケットの正当性を検証する。利用履歴精算部108は、チケット有効性判定部106によりチケットが有効であると判定され、かつチケット検証部107によりチケットが正当であると検証されたときに、精算を指定された利用履歴を精算するのに必要な正当なチケットが入力されたものとみなし、利用履歴指定部102により指定された利用履歴を精算済みとする。

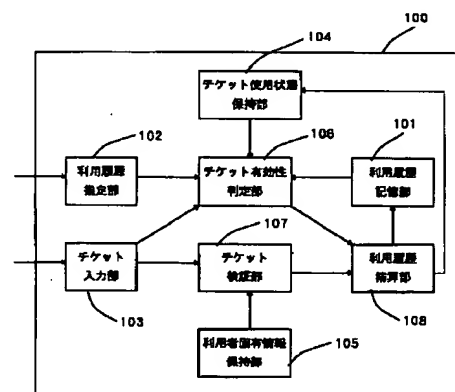


図1の実施例における電子チケットシステムの構成

【特許請求の範囲】

【請求項 1】 利用履歴を記憶する利用履歴記憶手段と、
 精算する上記利用履歴を指定する利用履歴指定手段と、
 精算に使用するチケットを入力するチケット入力手段と、
 利用者固有情報を保持する利用者固有情報保持手段と、
 上記チケットの有効性を判定するチケット有効性判定手段と、
 上記チケットと上記利用者固有情報とを用いて上記チケットの正当性を検証するチケット検証手段と、
 上記チケット有効性判定手段により上記チケットが有効であると判定され、かつ上記チケット検証手段により上記チケットが正当であると検証されたときに、上記利用履歴指定手段により指定された利用履歴を精算済みとする利用履歴精算手段とを有することを特徴とする電子チケットシステム。

【請求項 2】 請求項 1 に記載の電子チケットシステムであって、
 上記チケット入力手段は、さらにチケットを識別するチケット識別子を含んで上記チケットを入力し、
 さらに上記チケットの使用状態を上記チケット識別子と対応づけて記憶するチケット使用状態保持手段を有し、
 上記チケット有効性判定手段は、上記使用状態保持手段に保持されている上記チケットの使用状態を用いて有効性の判定を行うことを特徴とする電子チケットシステム。

【請求項 3】 請求項 1 または 2 に記載の電子チケットシステムであって、
 上記チケット入力手段は、上記チケットの利用条件を示すチケット付加情報を含んで上記チケットを入力し、
 上記チケット有効性判定手段は、さらに上記チケット付加情報と上記利用履歴指定手段により指定された上記利用履歴とを判定材料に加えて上記チケットの有効性を判定し、
 上記チケット検証手段は、上記チケットと上記利用者固有情報と上記チケット付加情報とを用いて上記チケットの正当性を検証することを特徴とする電子チケットシステム。

【請求項 4】 請求項 1 ～ 3 のいずれかに記載の電子チケットシステムであって、
 上記チケット入力手段は、さらに上記チケットの作成に用いたチケットの秘密情報に対応するチケットの公開情報を含んで上記チケットを入力し、
 上記チケット検証手段は、上記チケットと上記利用者固有情報と上記チケット付加情報と上記チケットの公開情報とを用いて上記チケットの正当性を検証することを特徴とする電子チケットシステム。

【請求項 5】 請求項 4 に記載の電子チケットシステムであって、上記チケット検証手段は、上記チケットと上

記利用者固有情報と上記チケット付加情報と上記チケットの公開情報とを用いて上記チケットの秘密情報を算出し、上記チケットの秘密情報と上記チケットの公開情報とが対応していることを確認することをもって上記チケットが正当であると判定することを特徴とする電子チケットシステム。

【請求項 6】 利用履歴を記憶する利用履歴記憶手段と、
 精算する上記利用履歴を指定する利用履歴指定手段と、
 精算に使用するチケットの利用条件を示すチケット付加情報とチケットの公開情報とチケットを識別するチケット識別子とを入力するチケット利用条件入力手段と、
 乱数を生成し出力する乱数生成手段と、
 上記出力した乱数と精算に使用するチケットとにより計算された証明情報を入力する証明情報入力手段と、
 利用者固有情報を保持する利用者固有情報保持手段と、
 上記チケットの使用状態を上記チケット識別子と対応づけて記憶するチケット使用状態保持手段と、
 上記チケット付加情報と上記利用履歴指定手段により指定された上記利用履歴と上記チケット使用状態保持手段に保持されている上記チケットの使用状態とを用いてチケットの有効性を判定するチケット有効性判定手段と、
 入力された上記証明情報と上記利用者固有情報と上記チケット付加情報と上記チケットの公開情報と上記乱数とを用いて上記チケットの正当性を検証するチケット検証手段と、
 上記チケット有効性判定手段により上記チケットが有効であると判定され、かつ上記チケット検証手段により上記チケットが正当であると検証されたときに、上記利用履歴指定手段により指定された利用履歴を精算済みとする利用履歴精算手段とを有することを特徴とする電子チケットシステム。

【請求項 7】 請求項 1 ～ 6 のいずれかに記載の電子チケットシステムであって、上記電子チケットシステムは、内部のデータおよび処理手続きを外から観測することを困難ならしめる防御手段中に保持されていることを特徴とする電子チケットシステム。

【請求項 8】 請求項 1 ～ 7 のいずれかに記載の電子チケットシステムであって、上記電子チケットシステムは、ICカードなどの携帯可能な小型演算装置として構成されていることを特徴とする電子チケットシステム。

【請求項 9】 請求項 1 ～ 8 のいずれかに記載の電子チケットシステムであって、
 上記電子チケットシステムは、さらにチケット発行装置を有し、
 上記チケット発行装置は、
 上記利用者固有情報を保持する発行装置側利用者固有情報保持手段と、
 上記チケットの秘密情報を保持するチケット秘密情報保持手段と、

上記チケット付加情報を保持するチケット付加情報保持手段と、
上記発行装置側利用者固有情報保持手段に保持している上記利用者固有情報と上記チケット秘密情報保持手段に保持している上記チケットの秘密情報と上記チケット付加情報保持手段に保持している上記チケット付加情報とを用いてチケットを発行することを特徴とする電子チケットシステム。

【請求項10】 利用履歴が記憶された機器を用いて料金を精算する料金精算方法において、
精算する利用履歴を指定する利用履歴指定ステップと、
精算に使用するチケットを入力するチケット入力ステップと、
上記チケットの有効性を判定するチケット有効性判定ステップと、
上記チケット有効性判定ステップにおいて上記チケットが有効であると判定されるときに、上記利用履歴指定ステップにおいて指定された利用履歴を精算済みとする利用履歴精算ステップとを有することを特徴とする料金精算方法。

【請求項11】 利用履歴を記憶する利用履歴記憶ステップと、
精算する上記利用履歴を指定する利用履歴指定ステップと、
精算に使用するチケットを入力するチケット入力ステップと、
利用者固有情報を保持する利用者固有情報保持ステップと、
上記チケットの有効性を判定するチケット有効性判定ステップと、
上記チケットと上記利用者固有情報とを用いて上記チケットの正当性を検証するチケット検証ステップと、
上記チケット有効性判定ステップにおいて上記チケットが有効であると判定され、かつ上記チケット検証ステップにおいて上記チケットが正当であると検証されたときに、上記利用履歴指定ステップにおいて指定された利用履歴を精算済みとする利用履歴精算ステップとを有することを特徴とする料金精算方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、チケットやカードの作成、発行および利用の技術に関し、とくにチケットを用いて料金を精算する技術に関する。

【0002】

【背景技術】〔従来の技術〕乗車券、通行券、入場券、指定券、予約券、回数券、定期券、商品券、プリペイドカード、ポイントカード、会員証、通行証、許可証などは、それを保持する利用者が、それに応じた各々の権利を保持することを証明する。ここでは、これらをまとめてチケットと呼ぶ。一般にチケットは、権利を与える者

もしくはその代理人（以下ではまとめて発行者と呼ぶ）が発行して、利用者が保持管理する。従来、チケットは、紙やプラスチックなどへ印刷やエンボス加工などの処理を施すことで実現されていた。

【0003】このようなチケットをここでは紙チケットと呼ぶ。これに対して、近年では、発行者が利用者に与えた権利を特定できて、正しいチケットであることを検証できるという機能を持つ電子チケットを実現する試みがなされている。電子情報は、作成が容易であり、通信回線を通して送信できるという特徴を持つ。しかしながら、完全なコピーを簡単に作れるので、電子チケットを実現するには、偽造と複製による不正利用への対策が必要である。電子署名の技術を用いることにより偽造は防止できるが、複製の防止は困難であり、複製による不正利用を防止することが、電子チケットの実現にあたっての最大の課題となっていた。

【0004】この問題に対する、解決策として、従来、チケットの利用時に正当な利用者が確認する第1の従来技術、発行者以外の者にチケットを複写する機会を与えない第2の従来技術、検証時の通信を公開できるように第2の従来技術を修正した第3の従来技術の3つの方法が提案されてきた。

【0005】第1の従来技術は、チケットの利用時に、利用者が正当な利用者かどうかを確認する方法であり、利用者は、チケットを利用する時に、チケットとともに自分が利用者特定情報に適合する正当な利用者であることを示す。利用者特定情報に適合していれば、対応する権利の行使が認められる。確認のために必要な情報（利用者特定情報）と、与えた権利とを対応づける情報がチケットとして発行され、利用者が記録管理する。発行者以外の者が勝手にチケットを偽造できないようにするためには、発行者がチケットに電子署名を施す。電子署名のないチケットは、偽造されたものと判断される。利用者特定情報には、身元、顔写真などの身体的特徴、パスワードなどの知識の所有、などが利用できる。

【0006】しかしながらこの方法では、利用する利用者特定情報に応じて、いくつかの問題点が生ずる。

【0007】例えば、利用者特定情報に利用者の身元を利用する方法では、発行時と検証時に利用者の身元が明らかになり、匿名性が失われてしまう。また、通信回線を利用した遠隔的な環境で身分を安全に証明する方法は実現されていないので、このような環境では正当な権利を持たないものが、不当にチケットを利用することを防止することができない。

【0008】利用者特定情報にパスワードを利用すれば、匿名性の問題は軽減されるが、パスワードを記憶する負荷を利用者にあたえる。また、利用者が故意にパスワードを漏洩させることを防止できないので、不正利用の危険が増してしまうという問題点もある。

【0009】第2の従来技術は、例えば特開平8-14

10

20

30

40

50

7500号公報に示されるようなものであり、発行者以外の者にチケットを複写する機会を与えない方法である。この方法では、利用者が保持管理しているチケットを複写できないようにする機構と、発行時や検証時の通信からチケットが漏洩しない機構の両方を必要とする。

【0010】しかしながら、この方法では、(1)発行者以外の者はチケットを複写できないので、チケットの正当性を第三者に証明することが困難になる、(2)チケットの発行時と検証時の通信の内容も機密に行うので、チケットの発行時と検証時にプライバシーなどの利用者の権利が侵害されていないことを証明できない、といった問題点が生ずる。

【0011】第3の従来技術は、例えば特公平6-52518号公報に示されるようなものであり、検証時の通信を公開できるように第2の従来技術を修正した方法である。この方法では、第2の従来技術と同様に、チケットを秘密情報として利用者の所持する装置(証明器)に複写できないように記録するが、検証の方法が異なる。まず、検証を行う検証器は、証明器に乱数などの繰り返し利用されない値(チャレンジ)を送る。証明器は、チケットである秘密情報を利用した演算をチャレンジに対して施して、得られた値(レスポンス)を検証器に送り返す。検証器は、秘密情報とチャレンジを利用してレスポンスが演算されたことを確認することで、利用者の正当性を認証する。レスポンスから逆に秘密情報を求めることを計算量的に困難とすることで、チャレンジとレスポンスを秘密通信とする必要がなくなる。

【0012】この方法は、認証のために利用されるものであり、正当なチケットを保持しているか否か以外に情報を伝達しない。このため、有効期限などを示すことができず、単純なチケットしか表現できない。また、チケットを証明器に送信する方法が、第2の従来技術と同様に機密通信で行う必要があり、不当に利用者の情報を開示して利用者の権利を侵害していないことを証明できないという問題があった。

【0013】このように、従来の技術はいずれも、チケットに必要な不正利用を防止する機能を実現するために、第三者に対するチケットの内容証明の機能や利用者の匿名性を犠牲にしている点に問題があった。

【0014】[関連技術]これらの問題を解決する関連技術として、特願平9-188064号(平成9年7月14日出願、未公開)に示す方法が提案されている。この方法では、各利用者に、固有情報を封入した証明装置を持たせ、チケットはその証明装置固有情報とチケットの秘密情報とから生成して発行する。検証時には、検証装置が乱数などを用いて発行した値(チャレンジ)に対して、証明装置がチケットを用いて値(レスポンス)を検証器に送り返すことによって、正当なチケットを保持しているかどうかの検証を行う。正当なチケットと正当な証明装置の組みあわせのみが、正当なレスポンスを計

算することが可能になる。

【0015】この方法では、チケットは秘密情報が取り出せないように構成されており、また他の証明装置と組にして利用しようとしても、利用できないようになっている。また、証明装置が検証装置に送る値(レスポンス)には、利用者が持つ証明装置の証明装置固有情報や利用者自身の情報は含まれることがないように構成できるので、利用者の匿名性も保つことが可能である。さらに、検証は、公開情報のみを用いて行うことが可能なので、利用者自身や第三者がチケットの正当性を確認することが可能である。

【0016】このように、この関連技術の方法を使うと、電子チケットの基本的な機能をすべて満たした安全な電子チケットを実現することができ、上記の問題をすべて解決することが可能である。

【0017】ところで、この関連技術では、検証器がチケットを特定する情報を証明器に送る事により、検証器が検証しようとするチケットが証明器の中で一意に定まる事を前提としている。しかし、実際には、その検証器で検証可能なチケットが証明器内に複数存在する事も考えられる。そのような場合には、検証の途中で選択肢が複数あることを示し、利用者に選択してもらうなどの処理を行うことを想定している。しかし、その検証器で検証可能なチケットが証明器内に複数存在し、かつその場で利用者が選択できないこともある。

【0018】たとえば、鉄道の乗車券のようなものを考えた場合、その駅から有効な回数券や定期券など複数のチケットが証明器の中に存在する事がありうる。そのような場合、証明器では、どのチケットを利用者が利用しようとしているのか判断する事ができない。また、鉄道の場合、自動改札機による処理にすると、短時間に大勢の人が通過できるようにしなければならないため、改札機による検証の途中で、利用者にチケットの選択を促すというような処理を行うことはできない。また、改札機を通る前に、利用者に予め利用するチケットを選択しておいてもらうということも、選択を忘れる利用者は少なからずいることが予想されるため、困難である。

【0019】そこでこのような場合には、検証器が検証しようとするチケットが証明器の中で一意に定まるようにする必要がある。

【0020】チケットが証明器の中で一意に定まるようにするには、何でも検証できる万能のチケットを1枚だけ証明器の中に保持しておき、検証の際にはその万能チケットを用いて検証を行い、検証の履歴を証明器の中に残すようにすればよい。そして、その精算はブリペイドのような前払い方式か、あるいは一定期間毎に履歴を回収して精算する後払い方式を取るようにすればよい。

【0021】しかし、このような方式を採用した場合、チケットを予め購入することによって行われていたディスプレイカウンタなどの機能が失われることになる。たとえ

ば、定期券や回数券などのボリュームディスカウントや、半年前に購入すると50%引きで、3ヶ月前なら30%引きというような前売りによるディスカウントなどの機能である。

【0022】

【発明が解決しようとする課題】そこで、本発明では、例えば、万能チケットを用いて検証を行い、検証の履歴を証明器の中に残すような場合の精算時において、チケットを予め購入することによって行われていたディスカウントなどの機能を失うことなく、精算可能にすることを課題とする。もちろん、万能チケットを用いた場合だけでなく、一般に利用の履歴を記録して、その記録を精算する際にも、使える精算機能であってもよい。

【0023】

【課題を解決するための手段】本発明では、上記の課題を解決するために、電子チケットシステムに、利用履歴を記憶する利用履歴記憶手段と、精算する上記利用履歴を指定する利用履歴指定手段と、精算に使用するチケットを入力するチケット入力手段と、利用者固有情報を保持する利用者固有情報保持手段と、上記チケットの有効性を判定するチケット有効性判定手段と、上記チケットと上記利用者固有情報とを用いて上記チケットの正当性を検証するチケット検証手段と、上記チケット有効性判定手段により上記チケットが有効であると判定され、かつ上記チケット検証手段により上記チケットが正当であると検証されたときに、上記利用履歴指定手段により指定された利用履歴を精算済みとする利用履歴精算手段とを設けるようにしている。

【0024】この構成においては、利用時には、単に、その利用履歴を記録しておき、後に、チケットを用いて精算するので、利用時の操作が少なくなる。また、精算時にチケットの有効性を判断するので、チケットの利用条件やディスカウントを反映させて精算を行なうことができる。

【0025】

【発明の実施の態様】以下、本発明の実施例について説明する。

【第1の実施例】第1の実施例では、回数券を表すチケットで利用履歴を精算する例について説明する。この実施例の電子チケットシステムは、例えばICカードとして実現され、利用者はそのICカードを持って何らかのサービスを利用し、その利用履歴をICカード中に記録する。そして後で、自宅のパソコンなどにそのICカードを挿入し、パソコン上に保持しているチケットを用いて、利用履歴の精算を行う。利用履歴を記録する手法は、利用の許可を行う検証器側と何らかの認証を行い、その結果として記録されるのが望ましいが、利用したことが正しく反映されていれば何でもよい。例えば、この認証の手段としてチケットを用いてもよい。チケットを用いる方法としては、先の特願平9-188064号に

示す方法や、特願平10-027074号に示す方法を用いてもよい。特願平9-188064号は検証器側と証明器側との間で相互認証し、証明器の保持者にサービス等を提供し、そのサービスに応じて証明器の内部状態（利用履歴）を書き込み更新できるようにしている。また、特願平10-027074号では、相互認証に加え、検証器側で、証明器から提示されたチケットの判定を行ない、間違ったチケットの提示や不正なチケットの提示により証明器の内部状態が変更されないようにしている。

【0026】この場合、利用・履歴記憶時に第1のチケットを使い、また、精算時に第2のチケットを使う。以下の説明は精算時のチケットに関するものである。

【0027】図1は、本発明の第1の実施例の電子チケットシステムを全体として示しており、この図において、電子チケットシステム100は、利用履歴記憶部101、利用履歴指定部102、チケット入力部103、チケット使用状態保持部104、利用者固有情報保持部105、チケット有効性判定部106、チケット検証部107、利用履歴精算部108を含んで構成される。

【0028】利用履歴記憶部101は、利用の履歴を記憶する部分である。利用の履歴は、例えば自動改札機などにより改札がなされたときに、書き込まれるものである。利用履歴指定部102は、利用履歴記憶部101に記憶されている利用履歴の中から、チケットにより精算する利用履歴を指定するものである。チケット入力部103は、精算するのに使用するチケットを入力する部分である。本実施例では、チケットとともに、チケットを識別するチケット識別子と、チケットの利用条件を示すチケット付加情報と、チケットの作成に用いたチケットの秘密情報に対応するチケットの公開情報とを入力する。

【0029】チケット使用状態保持部104は、チケットの使用状態をチケット識別子と対応づけて記憶する。チケットの使用状態とは、例えば今までにそのチケットを使用した回数などである。これを用いて、例えば、回数券の使用回数をカウントしておき、その回数券の使用限度になるとそれ以上、使用できないような処理を行う。また、回数券以外でも、同じチケットの再利用を防止する意味からも用いられる。

【0030】利用者固有情報保持部105は、利用者毎に個別に割り当てられた利用者の固有情報を保持する。利用者固有情報は、ICカードなどの中に秘密に封入されており、利用者自身も読み出すことはできない。

【0031】チケット有効性判定部106は、チケットの有効性を判定する。より具体的には、チケット有効性判定部106は、使用状態保持部104に保持されているチケットの使用状態と、入力されたチケット付加情報と、利用履歴指定部102により指定された利用履歴とを用いてチケットの有効性を判定する。例えば、回数券

チケットのチケット付加情報に記載されている回数上限と使用状態保持部104に保持されているチケットの使用回数とを比較して上限を超えていないかで判定したり、チケット付加情報に記載されている乗車可能区間と精算する利用履歴として記録されている実際の乗車区間とを比較したり、チケット付加情報に記載されているチケットの有効期間と精算する利用履歴として記録されている実際の使用日時とを比較したりして判定する。

【0032】チケット検証部107は、入力されたチケットと利用者固有情報とチケット付加情報とチケット公開情報とを用いてチケットの正当性を検証する。

【0033】利用履歴精算部108は、チケット有効性判定部106によりチケットが有効であると判定され、かつチケット検証部107によりチケットが正当であると検証されたときに、精算を指定された利用履歴を精算するのに必要な正当なチケットが入力されたものとみなし、利用履歴指定部102により指定された利用履歴を精算済みとする。精算済みとする方法としては、単に利用履歴を利用履歴記憶部101から削除してもよいし、利用履歴記憶部101で記憶している各利用履歴に未精算か精算済みかを示すフラグを持たせ、対応する履歴の精算済みのフラグを立てるようにしてもよい。

【0034】次に本実施例の動作を図4のフローチャートを参照しながら具体例を挙げて詳細に説明する。この説明では、チケットの作成時に用いるチケット秘密情報として、公開鍵暗号方式のRSA(Rivest-Shamir-Adleman)暗号を用いた例について説明する。

【0035】RSA暗号では、 p 、 q を大きな素数、 n を法数、 E を公開鍵、 D を秘密鍵とすると、以下の関数30

利用可能区間： 横浜－藤沢

有効期間： 1997. 5. 1～1997. 10. 31

回数上限： 11回

上記のようなチケット付加情報を $L301$ とし、この $L301$ を用いて発行されたチケットを $t301$ とする。利用者固有情報を $d003$ とし、このチケットに用いられているチケット秘密情報を $D01$ 、対応するチケット公開情報を $(E01, n01)$ とすると、発行されるチケット $t301$ は以下のようになる。

【0042】

【数3】

$t301 = D01 - F(n01, L301, d003)$
このチケットは現在3回使用されているとすると、チケット使用状態保持部は図3に示すように、チケット識別子が003の使用回数が「3」となっている。

【0043】さて、今、横浜－藤沢間の鉄道に乗車した利用履歴を、回数券チケットで精算するために、利用履歴指定部102からNo. 214の履歴が指定され、チケット入力部103から、チケット $t301$ とチケット付加情報 $L301$ とチケット識別子003とチケット公

*係が成り立つ。 p 、 q を大きな素数、 n を法数とすると、

【0036】

【数1】

$n = p \cdot q$

$ED \equiv 1 \pmod{(p-1)(q-1)}$

このうち、素数 p 、 q は秘密に作成して、チケットの作成が終了し次第、秘密のまま破棄してしまう。

【0037】本実施例では、具体例として、横浜－藤沢間の鉄道に乗車した利用履歴を、回数券チケットで精算する場合について説明する。

【0038】今、利用履歴記憶部101の内容が図2のようになっているとする。このうちの、No(通し番号)が214の履歴を、回数券で精算する。上述したRSAを用いて、チケット秘密情報を D 、チケット公開情報を (E, n) とし、利用者固有情報を du 、チケット付加情報を L とする。この時、チケット入力部103から入力されるチケット t は以下のような形式である。

【0039】

【数2】 $t = D - F(n, L, du)$

ここで、関数 $F()$ は一方方向性関数であり、一方方向性ハッシュ関数MD5、SHAや、共通鍵暗号DES(Data Encryption Standard)などを用いることができる。

【0040】チケット付加情報 L には、利用可能区間、有効期間、回数上限などが記載されており、今それらの情報は以下のようにになっている。

【0041】

【表1】

公開情報 $(E01, n01)$ とが入力されたとする(図4のステップS11)。するとチケット有効性判定部106は、利用履歴記憶部101から指定されたNo. 214の履歴を読み出し、チケット付加情報 $L301$ と比較する(S12、S13)。No. 214の履歴の利用区間は横浜－藤沢間であり、利用日時は「97. 9. 10」である。一方、チケット付加情報 $L301$ の利用可能区間も横浜－藤沢間であり、有効期間は1997. 5. 1～1997. 10. 31であることから、利用可能区間、有効期間ともにチケットの利用は可能である。

【0044】次に、チケット有効性判定部106は、チケット使用状態保持部104からチケット識別子003の使用状態を読み出し、チケット付加情報 $L301$ と比較する。チケット識別子003の使用状態(ここでは使用回数)は3回であり、チケット付加情報 $L301$ の回数上限は11回であるので、チケットの利用は可能である。ここで、チケット使用状態保持部104から読み出

した使用回数が11回を示していた場合は、チケットは使用不能であると判定する。

【0045】上述の2つのチケット有効性の判定により、チケットの利用は可能であるので、チケット有効性判定部106はチケットを有効であると判定する。

【0046】次にチケット検証部107による検証を行う。チケット検証部107は、利用者固有情報保持部105から利用者固有情報d003を読み出し、チケット入力部103から入力されたチケットt301とチケット付加情報L301とチケット公開情報(E01, n01)とを用いて検証を行う(S14、S15)。

【0047】検証は例えば以下の方法で行う。

【0048】ある整数aを生成し、aの法nのもとでの $[t + F(n, L, du)] \cdot E$ によるべき乗を計算し、aと等しくなるかどうかで検証する。

【0049】

【数4】

$$a^{[t + F(n, L, du)] \cdot E} \bmod n = ? \quad a \quad (1)$$

正しいチケットと正しい利用者固有情報を用いれば、

【0050】

【数5】

$$[t + F(n, L, du)]$$

$$= D - F(n, L, du) + F(n, L, du)$$

$$= D$$

であるので、

【0051】

【数6】

$$a^{[t + F(n, L, du)] \cdot E} \bmod n$$

$$= a^{DE} \bmod n$$

$$= a$$

と計算でき、(1)式が成立するはずである。

【0052】(1)式の左辺に、各値を代入すると、

$$[a^t a^{F(n, L, du)}]^E \bmod n = ? \quad a \quad (2)$$

本実施例では、回数券の例について説明したが、チケットが定期券の時には、回数のチェックはせずに、読み出した利用履歴を用いて区間と有効期間から有効性を判定すればいい。また、回数に関係のない場合でも、チケット使用状態保持部から読み出したチケットの使用状態の情報をを用いることで、一度しか使えないチケットを再使用することを防ぐことができる。

【0060】また、本実施例では、RSA公開鍵暗号方式を用いて説明したが、これに限定するものではない。例えば離散対数系の暗号方式も使用することが可能である。

【0061】例えば、pは素数であり、Gは離散対数問題が困難な有限群であり、gは有限群Gの位数pの元であり、

【0062】

$$[数8] \quad y = g^x \bmod p$$

が満たされるとき、(p, G, g, y)を公開の情報と

*【0053】

【数7】

$$a^{[t301 + F(n01, L301, d003)] \cdot E01} \bmod n01$$

$$= a^{D01 \cdot E01} \bmod n01$$

$$= a$$

となり、(1)式が成り立つので、チケットは正当であると検証される。

【0054】以上により、チケット有効性判定部106によりチケットが有効であると判定され、チケット検証部107によりチケットは正当であると検証されたので、利用履歴精算部108は、指定された利用履歴を精算済みと処理する。つまり、利用履歴精算部108は、利用履歴記憶部101に記憶されているNo. 214の履歴の精算記録の欄を、未精算から精算済みに変更する(S16)。

【0055】さらに、利用履歴精算部108は、チケット使用状態保持部104のチケット識別子が003の使用回数を1だけ増やして4に変更する(同じくS16)。

【0056】なお、図4のステップS12の有効性判別において有効でないと判別された場合や、ステップS14において検証が失敗した場合には精算が行なわれず、エラー等が表示される(S17)。

【0057】以上で、チケットによる利用履歴の精算処理は終了する。精算終了後の利用履歴記憶部の内容例を図5に示す。

【0058】本実施例では、チケットの正当性の検証に、(1)式を用いて検証したが、(2)式を用いてもよい。どちらも結果は同じである。

【0059】

【数8】

$$[a^t a^{F(n, L, du)}]^E \bmod n = ? \quad a \quad (2)$$

し、xを秘密の情報とする。実際には、Gを有限体の乗法群として構成したり、有限体上の楕円曲線として構成することができる。

【0063】このとき、(G, g)をシステム共通とし、公開情報(y, p)、秘密情報xとして、チケットを

【0064】

$$[数9] \quad t = x - F(y, L, du)$$

として構成することができる。ここで、関数FやLやduなどは、RSAの時と同様である。

【0065】検証は、(3)式が成立するかどうかで行えばよい。

【0066】

【数10】

$$g^{[t + F(y, L, du)]} \bmod p = ? \quad y \quad (3)$$

正しいチケットと正しい利用者固有情報を用いれば、

【0067】

【数11】

$[t + F(y, L, du)]$

$= x - F(y, L, du) + F(y, L, du)$

$= x$

であるので、

【0068】

【数12】

$g^{[t + F(y, L, du)]} \bmod p$

$= g^x \bmod p$

$= y$

と計算でき、(3)式が成立するはずである。チケットの式は、

【0069】

【数13】 $t = x - F(p, L, du)$

のようにしても構わない。

【0070】【第2の実施例】以下、本発明の実施例について説明する。

【0071】図6は、本発明の第2の実施例の電子チケットシステムを全体として示す図であり、図6において、電子チケットシステム100は、利用履歴記憶部101、利用履歴指定部102、チケット利用条件入力部109、チケット使用状態保持部104、利用者固有情報保持部105、チケット有効性判定部106、チケット検証部107、利用履歴精算部108、乱数生成部110、証明情報入力部111を含んで構成される。

【0072】チケット利用条件入力部109は、利用するチケットに関連する条件などを入力する部分である。*

$$[r^t r^{F(n, L, du, t-id)}]^E \bmod n = ? \quad r \quad (4)$$

(4)式の左辺の r^t は、証明情報入力部111から入力された値を用いる。左辺のそれ以外の部分は、チケット利用条件入力部109から入力された値と利用者固有情報保持部105に保持している値を用いて計算する。

【0080】本実施例におけるチケット t は以下のような形式である。

$$\begin{aligned} & r^t r^{F(n, L, du, t-id)}]^E \bmod n \\ &= [r^{D-F(n, L, du, t-id)} r^{F(n, L, du, t-id)}]^E \bmod n \\ &= [r^{D-F(n, L, du, t-id)+F(n, L, du, t-id)}]^E \bmod n \\ &= [r^D]^E \bmod n \\ &= r^{D^E} \bmod n \\ &= r \end{aligned}$$

つまり、(4)式の左辺と右辺とが等しくなり、(4)式が成り立つ。

【0083】第1の実施例と異なり、一方向性関数 $F()$ の中にチケット識別子 $t-id$ を入れているのは、チケット識別子だけを入れ替えるような偽造を防ぐためである。この偽造は第1の実施例でも行われる可能性があるため、第1の実施例でも同様の形式にしてもよい。

【0084】これ以外は第1の実施例と同様であるので、説明を繰り返さない。

*本実施例では、チケットを識別するチケット識別子と、チケットの利用条件を示すチケット付加情報と、チケットの作成に用いたチケットの秘密情報に対応するチケットの公開情報とを入力する。

【0073】乱数生成部110は、乱数を生成し、出力する。

【0074】証明情報入力部111は、乱数生成部110が出力した乱数と精算に使用するチケットとにより計算された証明情報を入力する。精算に使用するチケットは、本電子チケットシステムの外部で保持されており、そのチケットを用いて証明情報が計算される。

【0075】例えば、乱数生成部110が乱数 r を生成したとし、精算に使用するチケットが t 、法数が n であるとすると、証明情報入力部111からは、

【0076】

【数14】 $r^t \bmod n$

が入力される。

【0077】他の部分は第1の実施例と同様に構成される。

【0078】乱数生成部110が出力した乱数を r 、精算に使用するチケットを t 、一方向性関数を $F()$ 、チケット公開情報を (E, n) 、チケット付加情報を L 、利用者固有情報を du 、チケット識別子を $t-id$ とすると、第2の実施例における検証は(4)式が成立するかどうかで検証する。

【0079】

【数15】

※【0081】

【数16】 $t = D - F(n, L, du, t-id)$
正しいチケットと正しい利用者固有情報を用いれば、(4)式の左辺は、以下のように計算される。

【0082】

【数17】

【0085】この実施例においては、チケット自体を入力することなく、乱数生成部110が出力した乱数に対してチケットでべき乗を行った計算結果を入力するようにしている。一般に、べき乗の計算は大きな計算量を必要とする。チケット t の長さ(ビット長)が大きくなることが考えられるため、 r^t の計算には大きな計算量が必要となる。

【0086】この実施例では、この r^t の計算を一般に貧弱な計算能力しか持たないICカードで行わずに、外部のパーソナルコンピュータの計算リソースを用いて行

うように構成することができ、第 1 の実施例の (2) 式を使う場合に比べて高速な検証を可能にすることができる。

【0087】

【発明の効果】以上説明したように、本発明によれば、利用時には、単に、その利用履歴を記録しておき、後に、チケットを用いて精算するので、利用時の操作が少なくなる。また、精算時にチケットの有効性を判断するので、チケットの利用条件やディスカウントを反映させて精算を行なうことができる。

【図面の簡単な説明】

【図 1】 第 1 の実施例における電子チケットシステムの構成を示すブロック図である。

【図 2】 第 1 の実施例における利用履歴記憶部の内容の例を示す図である。

【図 3】 第 1 の実施例におけるチケット使用状態保持部の内容の例を示す図である。

【図 4】 第 1 の実施例における処理の流れを示すフロ*

*ーチャートである。

【図 5】 第 1 の実施例における精算終了後の利用履歴記憶部の内容の例を示す図である。

【図 6】 第 2 の実施例における電子チケットシステムの構成を示すブロック図である。

【符号の説明】

100 電子チケットシステム
101 利用履歴記憶部
102 利用履歴指定部
103 チケット入力部
104 チケット使用状態保持部
105 利用者固有情報保持部
106 チケット有効性判定部
107 チケット検証部
108 利用履歴精算部
109 チケット利用条件入力部
110 乱数生成部
111 証明情報入力部

【図 2】

No	入場記録	出場記録	精算記録
211
212	97.9.5, 13:15 藤沢	97.9.5, 13:31 辻堂	未精算
213	97.9.8, 15:30 横浜	97.9.8, 16:21 東京	精算済み
214	97.9.10, 10:21 横浜	97.9.10, 10:55 藤沢	未精算
215	97.9.10, 18:17 藤沢	97.9.10, 18:28 辻堂	未精算
216	97.9.16, 12:15 藤沢	97.9.16, 12:29 辻堂	未精算
217

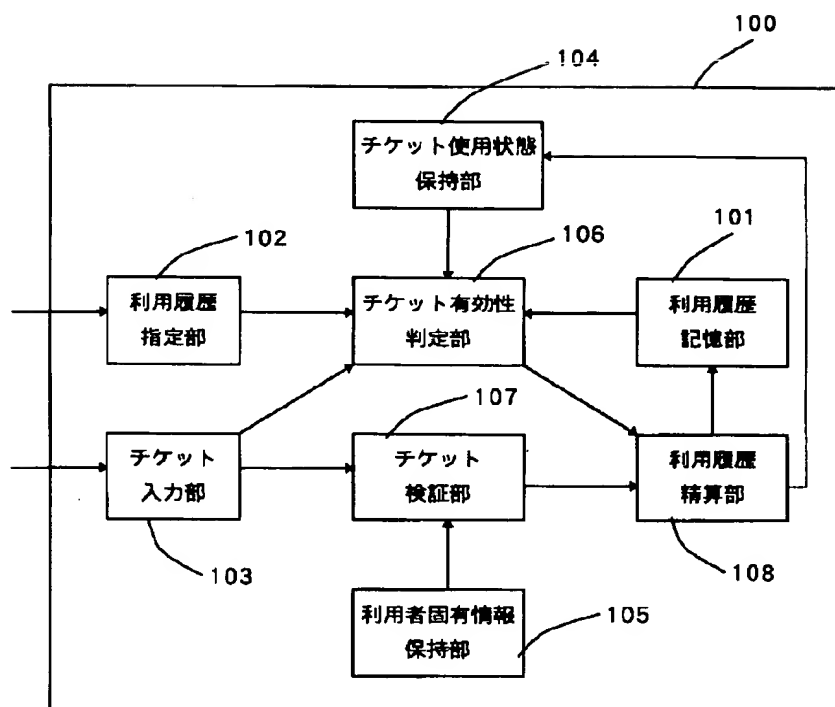
第 1 の実施例における利用履歴記憶部の例

【図 3】

チケット識別子	使用回数
001	5
002	1
003	3
004	1
...	...
...	...

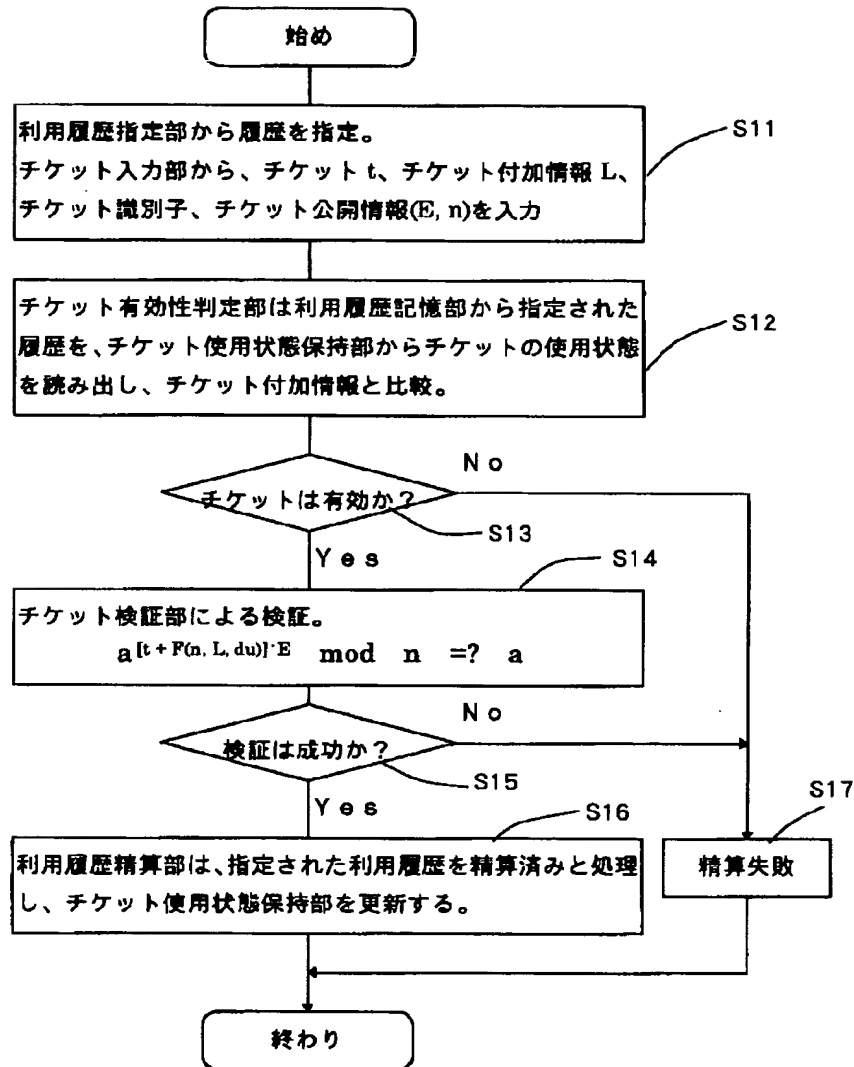
第 1 の実施例におけるチケット使用状態保持部の例

【図1】



第1の実施例における電子チケットシステムの構成

【図4】



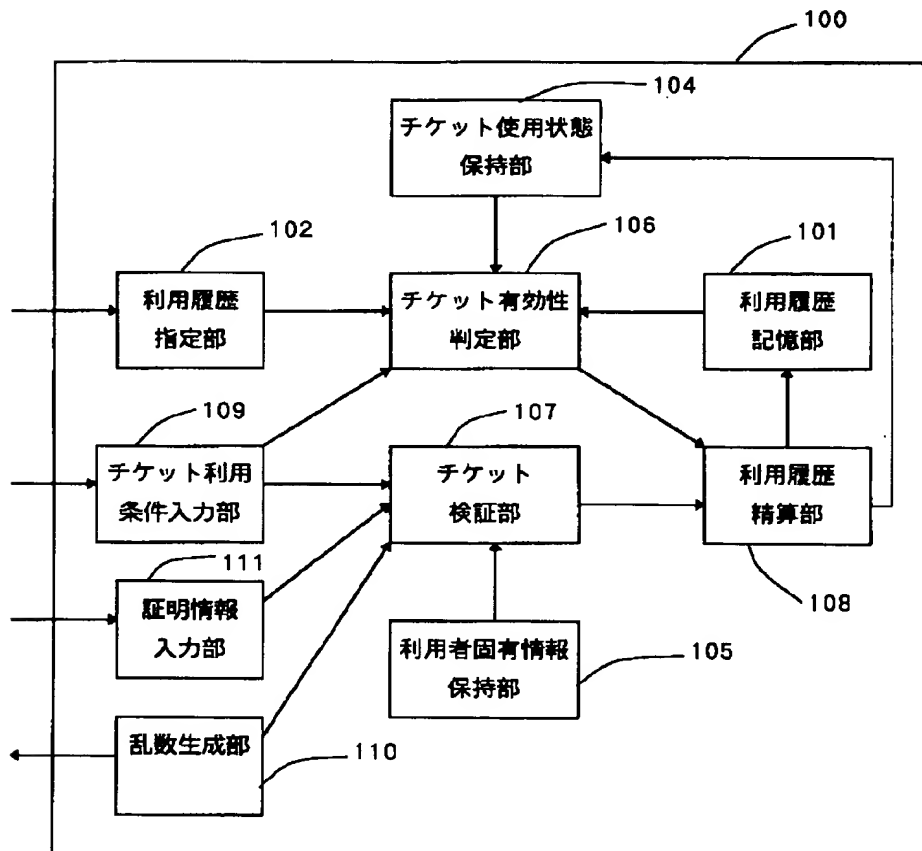
第1の実施例における処理の流れ

【図5】

No	入場記録	出場記録	精算記録
211
212	97.9.5, 13:15 藤沢	97.9.5, 13:31 辻堂	未精算
213	97.9.8, 15:30 横浜	97.9.8, 16:21 東京	精算済み
214	97.9.10, 10:21 横浜	97.9.10, 10:55 藤沢	精算済み
215	97.9.10, 18:17 藤沢	97.9.10, 18:28 辻堂	未精算
216	97.9.16, 12:15 藤沢	97.9.16, 12:29 辻堂	未精算
217

第1の実施例における精算終了後の利用履歴記憶部の例

【図6】



第2の実施例における電子チケットシステムの構成

フロントページの続き

(72)発明者 谷口 慎一郎
神奈川県足柄上郡中井町境430 グリーン
テクなかい 富士ゼロックス株式会社内